AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-63 (Cancelled)

64. (Currently amended) A method of storing a data set on a storage device ~~carrying a file of random data comprising the steps of~~ having one or more portions of random data, comprising:

~~selecting, in dependence on~~ determining, using a process dependent upon a user input passphrase, a first storage writing process starting location at a first offset within ~~the file~~ a portion of random data for initiating a first storage writing process for storing a file index;

~~selecting~~ determining a second storage writing process starting location at a second offset within ~~the file~~ a portion of random data for initiating a second storage writing process for storing the data set, said second offset determined using a process that is independent of a process used to generate said first offset;

encrypting the data set;

~~storing~~ writing the encrypted data set using the second storage writing process beginning at the second ~~selected~~ storage writing process starting location in ~~the file~~ a portion of random data;

~~making~~ creating a file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second ~~selected~~ storage writing process starting location;

encrypting the file index; and

~~storing~~ writing the encrypted file index using the first storage writing process beginning at the first ~~selected~~ storage writing process starting location in the file of random data.

65. (Currently amended) A method of operating a computer to store a data set on a storage device, ~~carrying a file of random data, the method~~ comprising ~~the steps of~~:

~~selecting, in dependence on a user input passphrase,~~ determining a first location within ~~the file of random data for~~ the storage device for initiating a first storage writing process for storing a file index;

~~selecting~~ determining a second storage writing process starting location at a second offset within the ~~file of random data for~~ storage device for storing the data set, said second offset determined using a process that is independent of a process used to generate said first offset;

encrypting the data set;

~~storing~~ writing the encrypted data set using the second storage writing process beginning at the second ~~selected~~ storage writing process starting location in ~~the file~~ a portion of random data;

~~making~~ creating a file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second ~~selected~~ storage writing process starting location;

encrypting the file index; and

~~storing~~ writing the encrypted file index using the first storage writing process beginning at the first ~~selected~~ storage writing process starting location ~~in the file of random data~~.

66. (Currently amended) The method according to claim 64 in which ~~the step of selecting~~ determining the first storage writing process starting location for ~~storing~~ creating the file index comprises ~~the step of selecting~~ adding a predetermined offset to the first storage writing process starting location as a ~~start point~~ beginning of the file index.

67. (Currently amended) The method according to claim 64 ~~further including storing~~ wherein the encrypted file index ~~at the first location~~ is stored only within ~~the file of random data, by replacing a respective portion of the file~~ the portions of random data on the device.

68. (Currently amended) The method according to claim 64 in which ~~the~~ an encrypted file index is stored ~~at the first location within the file of~~ within one or more portions of random data by ~~processing~~ writing over random data portions within the ~~file of random data using the~~ storage device with encrypted file index data.

69. (Currently amended) The method according to claim 64 ~~further including storing~~ wherein the encrypted data set ~~at the second location within the file of random data, by replacing a respective portion of the file of~~ is stored only within the portions of random data.

70. (Currently amended) The method according to claim 64 in which ~~the~~ an encrypted data set is stored ~~at the second selected location in the file of~~ within one or more portions of random data by ~~processing~~ writing over random data portions within the ~~file of random data using the~~ storage device with the encrypted data set.

71. (Currently amended) The method according to claim 64 which further comprises ~~a step of~~ using the user input passphrase for generating a key for encrypting the file index.

72. (Previously presented) The method according to claim 64 in which the passphrase is used for generating a key for encrypting the data set.

73. (Currently amended) The method according to claim 64 in which the passphrase is used in selecting the second storage writing process starting location ~~within the file of random data~~.

74. (Previously presented) The method according to claim 64 in which at least one of the first location within the file of random data, the second location within the file of random data, a key for the file index and a key for the data set is determined by using at least one hash function to operate on the user input passphrase.

75. (Previously presented) The method according to claim 64 in which the passphrase is operated on once to produce an output which is used for determining at least two of the first location within the file of random data, the second location within the file of random data, a key for the file index and a key for the data set.

76. (Previously presented) The method according to claim 64 in which the passphrase is operated on a plurality of times, each operation generating an output for use in determining at

least one of the first location within the file of random data, the second location within the file of random data, a key for the file index and a key for the data set.

77. (Previously presented) The method according to claim 64 in which a common key is used for encrypting the data set and for encrypting the file index.

78. (Previously presented) The method according to claim 64 which comprises a step of storing further sets of data using said passphrase.

79. (Previously presented) The method according to claim 78 which is such that a respective location for each data set is selected, each data set is encrypted and stored at the respective location, and respective entries are added to the file index.

80. (Previously presented) The method according to claim 64, comprising a step of storing further file indexes within the file of random data, each of which indexes is associated with a respective passphrase and each of which indexes is encrypted and is stored at a location selected in dependence on the respective passphrase.

81. (Previously presented) The method according to claim 80 in which respective encryption keys are generated from the respective passphrases and these respective keys are used for encrypting data sets which are associated with each file index.

82. (Previously presented) The method according to claim 80 comprising a step of selecting the passphrase for, and hence location for, an additional file index with knowledge of the respective passphrases corresponding to file indexes already stored in the file of random data such that collisions may be avoided.

83. (Previously presented) The method according to claim 80, in which, where there are a plurality of file indexes stored in the file of random data, the method comprises a step of selecting a location for an additional data set with knowledge of the respective passphrases corresponding to file indexes already stored in the file of random data such that collisions may be avoided.

84. (Previously presented) The method according to claim 80 comprising a step of storing additional data sets using a passphrase whilst in ignorance of at least one other existing passphrase.

85. (Previously presented) The method according to claim 80 comprising a step of storing data sets in a predetermined relationship to a respective file index to help prevent collisions, for example data sets may be stored adjacent to a respective file index, data sets may be stored substantially contiguously to a respective file index, and data sets may be stored at locations close to but after a respective file index.

86. (Previously presented) The method according to claim 64 comprising a step of storing data on a storage device carrying a plurality of files of random data.

87. (Previously presented) The method according to claim 64 in which the file index comprises a message authentication code.

88. (Previously presented) The method according to claim 87 in which the file index comprises a message authentication code of all associated data sets so as to facilitate detection of tampering.

89. (Previously presented) The method according to claim 87 in which the file index comprises a message authentication code of the file of random data in its entirety for use in detecting other usage of the file of random data.

90. (Previously presented) The method according to claim 64 comprising a step of pre processing the data set prior to encryption.

91. (Previously presented) The method according to claim 64 comprising a step of presenting a user with an indication of a location within the file of random data that will be selected for the file index when using a predetermined passphrase.

92. (Previously presented) The method according to claim 91 comprising a step of accepting user entered trial passphrases and providing a user with an indication of a location within the file of random data that will be selected for the file index for each trial passphrase.

93. (Previously presented) The method according to claim 91 comprising a further step of providing to a user an indication of the regions of the file of random data that are already occupied by file indexes having passphrases that have been supplied by a user.

94. (Previously presented) The method according to claim 64 comprising a step of receiving an indication from a user of a location within the file of random data which a user desires to use for a file index.

95. (Previously presented) The method according to claim 94 comprising the step of suggesting possible passphrases to a user in response to a user indicating a location within the file of random data which a user desires to use for a file index.

96. (Previously presented) The method according to claim 94 comprising steps of receiving a user input passphrase and suggesting a modified passphrase.

97. (Previously presented) The method according to claim 96 in which the modification of the passphrase is selected so as to at least one of: move a location at which an associated index would be stored towards a desired location indicated by a user and strengthen the passphrase.

98. (Previously presented) The method according to claim 64 comprising a step of deleting a data set stored on a storage device.

99. (Previously presented) The method according to claim 98 comprising a step of removing a respective entry from the file index.

100. (Previously presented) The method according to claim 99 in which the step of deleting a data set comprises a step of overwriting the data set with random data as well as removing the entry from the file index.

101. (Previously presented) The method according to claim 98 comprising a step of reorganizing data stored in association with a file index when at least one data set referenced in that file index is deleted.

102. (Previously presented) The method according to claim 100 in which the step of overwriting the data set comprises a step of using at least one random data and encrypted data stored in the file of random data for generating pseudo-random data for overwriting deleted files.

103. (Previously presented) The method according to claim 102 in which the method comprises a step of using random numbers from the file of random data that would be overwritten when adding a data set to replace any pseudo-random values previously used elsewhere within the file of random data.

104. (Currently amended) A computer storage device ~~comprising~~ for steganographically concealing stored information, said device configured with at least one storage area ~~storing a file of random data~~ having one or more portions of random data ~~with~~ containing a file index and a

predetermined data set ~~being stored in the file of random data~~, wherein the file index is encrypted and is stored at a first location determined by ~~a~~ an algorithmic process dependent upon a user passphrase, and the data set is encrypted and is stored at a second location determined using a process that is unconstrained by the process used to determine the first location, and the file index comprises ~~an entry in respect of the data set, the entry comprising an indication~~ information indicative of the second location.

105. (Currently amended) The storage device according to claim 104 ~~carrying~~ further including application software stored thereon for ~~use~~ execution by a computer ~~in storing and extraction~~ to enable steganographic storage extraction of data sets in the ~~file~~ one or more portions of random data.

106. (Currently amended) The storage device according to claim 104 in which the passphrase ~~has been~~ is used to generate a key for at least one of encrypting the file index and encrypting the data set.

107. (Currently amended) The storage device according to claim 104 further comprising a ~~in which~~ software ~~carried~~ application stored by the storage device ~~comprises~~, the software comprising instructions that when loaded and ~~run~~ executed by a computer~~,~~ cause the computer to ~~carry out~~ perform at least one of the following ~~steps~~ operations:

accepting a plurality of user input passphrases~~,~~ and generating corresponding encryption/decryption keys~~,~~;

~~and~~ determining respective storage writing process starting locations for a plurality of storage of file indexes;

encrypting a plurality of file indexes;

encrypting a plurality of data sets;

storing a plurality of file indexes;

~~selecting~~ determining respective storage writing process starting locations for storing a plurality of data sets;

storing a plurality of data sets;

accepting one or more user input passphrases and using said one or more user input passphrases for locating and decrypting respective file indexes;

locating one or more encrypted data sets stored within the storage device;

~~and~~ decrypting one or more encrypted data sets stored within the storage device ~~data sets~~; and

~~retrieving~~ outputting one or more decrypted data sets stored within the storage device as an encrypted data set.

108. (Currently amended) The storage device according to claim 104 ~~which~~ further ~~carries~~ including a conventional file allocation table stored thereon.

109. (Currently amended) The storage device according to claim 104 wherein at least ~~which comprises~~ a portion of the device comprises a Read Only Memory (ROM).

110. (Currently amended) The storage device according to claim 108 ~~which comprises~~ further comprising a Read Only Memory (ROM) portion ~~that carries~~ wherein is stored the file allocation table, the software and an operating system header file ~~for the file of random data~~.

111. (Currently amended) The storage device according to claim 104 ~~which~~ wherein the device is operable as a removable storage device.

112. (Currently amended) The storage device according to claim 104 ~~having~~ wherein the device is assigned a ~~unique~~ particular identifying serial number.

113. (Currently amended) The storage device according to claim 104 ~~which carries~~ further including a unique hard coded identifier data stored in memory contained therein, ~~which is used in~~ said identifier data for use by a computer for at least one of:

a) an encryption process used for encrypting at least one of the file index and the data; and

b) a decryption process used for decrypting at least one of the file index and the data.

114. (Currently amended) The storage device according to claim 104 ~~which is sold with a pretext for at least one use~~ wherein the storage device has the appearance of a conventional portable memory storage device.

115. (Currently amended) A computer arranged under the control of software, said computer executing software instructions for steganographically storing a data set on a storage

device ~~carrying a file of~~ within one or more portions of random data contained on said storage device, said computer ~~performing steps of~~comprising:

~~selecting, in dependence on a user input passphrase,~~programmable logic circuitry configured to determine a first location within ~~the file of random data for~~ the storage device for initiating a first storage writing process for storing a file index;

~~selecting~~ programmable logic circuitry configured to determine a second storage writing process starting location at a second offset within the ~~file of random data for~~ storage device for storing the data set;

~~encrypting~~ programmable logic circuitry configured to encrypt the data set;

~~storing~~ programmable logic circuitry configured to write the encrypted data set using the second storage writing process beginning at the second ~~selected~~ storage writing process starting location in ~~the file~~ a portion of random data;

~~making~~ programmable logic circuitry configured to create a file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second ~~selected~~ storage writing process starting location;

~~encrypting~~ programmable logic circuitry configured to encrypt the file index; and

~~storing~~ programmable logic circuitry configured to write the encrypted file index using the first storage writing process beginning at the first ~~selected~~ storage writing process starting location in the file of random data.

116. (Currently amended) The computer according to claim 115 ~~which is arranged under the control of~~ further comprising programmed logic circuitry configured by said software to ~~present~~ provide a user with an indication of a location within ~~the file~~ a portion of random data

that will be ~~selected~~ used for storing the file index ~~when using~~ corresponding to a particular ~~a~~ ~~predetermined~~ passphrase input by a user.

117. (Previously presented) The computer according to claim 115 which is arranged under the control of software to accept user entered trial passphrases and provide a user with an indication of a location within the file of random data that will be selected for storing the file index for each trial passphrase.

118. (Previously presented) The computer according to claim 115 which is arranged under the control of software to provide a user an indication of regions of the file of random data that are already occupied by file indexes having passphrases that have been supplied by a user.

119. (Previously presented) The computer according to claim 115 which is arranged under the control of software to suggest possible passphrases to a user in response to a user indicating a location within the file of random data which a user desires to use for storing a file index.

120. (Previously presented) The computer according to claim 116 which is arranged under the control of software to present a user interface for displaying the indications.

121. (Previously presented) The computer according to claim 120 in which the user interface is arranged so that a user can use a pointing device to indicate a location within the file of random data which a user desires to use for storing a file index.

122. (Currently amended) A method of extracting a data set steganographically stored on a storage device ~~carrying a file of~~ having one or more portions random data ~~with~~ containing a file index and a predetermined data set ~~being stored in the file of random data~~, wherein the file index is encrypted and is stored at a first location determined by ~~a~~ an algorithmic process dependent upon a user input passphrase, and the data set is encrypted and is stored at a second location determined using a process that is unconstrained by the process used to determine the first location, and the file index comprises ~~an entry in respect of the data set, the entry comprising an indication~~ information indicative of the second location, ~~the method of extracting data~~ comprising ~~the steps of~~:

~~accepting~~ using a user input passphrase~~;~~

~~determining~~ to determine a location for a file index ~~indicated by the~~ based upon the user input passphrase;

decrypting the file index;

identifying a location of a ~~requested~~ data set from the decrypted file index; and

decrypting the data set stored at the identified location.

123. (Previously presented) A computer arranged under the control of software to extract data using The method according to claim 122.

124. (Currently amended) A method of storing a data set on a storage device, ~~carrying a file of random data~~ comprising ~~the steps of~~:

~~selecting, in dependence on a user input passphrase,~~ determining a first location within ~~the file of random data for~~ the storage device for initiating a first storage writing process for storing a file index;

~~selecting~~ determining a second storage writing process starting location at a second offset within the ~~file of random data for~~ storage device for storing the data set, said second offset determined using a process that is independent of a process used to generate said first offset;

encrypting the data set;

~~storing~~ writing the encrypted data set using the second storage writing process beginning at the second ~~selected~~ storage writing process starting location in ~~the file~~ a portion of random data;

~~making~~ creating a file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second ~~selected~~ storage writing process starting location;

encrypting the file index; and

~~storing~~ writing the encrypted file index using the first storage writing process beginning at the first ~~selected~~ storage writing process starting location ~~in the file of random data~~, wherein the method further comprises ~~the further steps~~, prior to a user finalizing the user input passphrase, ~~of~~ accepting input of at least one user ~~entered~~ input trial passphrase and providing a user with an indication of a location within the ~~file of~~ portion of random data that will be ~~selected~~ determined for ~~the~~ creating a file index associated with the at least one user ~~entered~~ input trial passphrase.

125. (Currently amended) A computer readable data ~~carrier~~ storage medium, ~~carrying~~ said storage medium storing a computer program comprising code portions which when ~~loaded and run on~~ executed a computer cause the computer to ~~carry out the following steps~~ perform steps of:

~~selecting, in dependence on a user input passphrase,~~ determining a first location within ~~the file of random data for~~ the storage device for initiating a first storage writing process for storing a file index;

~~selecting~~ determining a second storage writing process starting location at a second offset within the ~~file of random data for~~ storage device for storing the data set, said second offset determined using a process that is independent of a process used to determine said first offset;

encrypting the data set;

~~storing~~ writing the encrypted data set using the second storage writing process beginning at the second ~~selected~~ storage writing process starting location in ~~the file~~ a portion of random data;

~~making~~ creating a file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second ~~selected~~ storage writing process starting location;

encrypting the file index; and

~~storing~~ writing the encrypted file index using the first storage writing process beginning at the first ~~selected~~ storage writing process starting location in the file of random data.

126. (Currently amended) A method of storing a data set on a storage device having one or more portions of a data storage area that are initialized with random data comprising the steps of:

~~selecting~~ determining a first writing process starting location within ~~the~~ a data storage ~~area~~ portion initialized with random data for ~~storing~~ creating a file index;

~~selecting~~ determining a second writing process starting location within ~~the~~ a data storage ~~area~~ portion initialized with random data for storing the data set, said second writing process starting location determined using a process that is unconstrained by a process used to determine said first writing process starting location;

encrypting the data set;

storing the encrypted data set beginning at the second ~~selected~~ writing process starting location, using only ~~in the~~ data storage ~~area~~ portions initialized with random data;

~~ensuring that an indication of the second selected location is determinable from the file index;~~

making an entry in the file index indicative of which portions of the data storage device initialized with random data are to be used to store the data set, wherein an indication of the second writing process starting location is determinable from the file index;

encrypting the file index; and

storing the encrypted file index at the first selected location in the data storage area initialized with random data~~, and comprising, before the step of encrypting the file index, a further step of recording in the file index an indication of which parts of the data storage area initialized with random data will be used to store said data set~~.

127. (Previously presented) The method according to claim 126 wherein the step of ensuring that an indication of the second selected location is determinable from the file index comprises the step of

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location.

128. (Previously presented) The method according to claim 126 wherein the step of selecting a first location within the data storage area initialized with random data for storing a file index, comprises

the step of selecting the first location from a plurality of predetermined possible locations within the data storage area initialized with random data, in dependence on one of: an input received from a user; and a selection process which is independent of user input.

129. (Previously presented) The method according to claim 126 wherein the step of selecting a first location within the data storage area initialized with random data for storing a file, comprises steps of selecting the first location in dependence on a user input passphrase and associating the file index with the user input passphrase.

130. (Previously presented) The method according to claim 129 wherein said data set is stored under protection of said user input passphrase and the method comprising a further step of storing a second data set on the storage device under protection of a second user input passphrase, the step of storing the second data set on the storage device comprising steps of:

selecting, in dependence on the second user input passphrase, a third location within the data storage area initialized with random data for storing a second file index;

selecting a fourth location within the data storage area initialized with random data for storing the second data set;

encrypting the second data set;

storing the encrypted second data set at the fourth selected location in the data storage area initialized with random data;

ensuring that an indication of the fourth selected location is determinable from the second file index;

encrypting the second file index; and

storing the encrypted second file index at the third selected location in the data storage area initialized with random data, and comprising, before the step of encrypting the second file index, a further step of recording in the second file index an indication of which parts of the data storage area initialized with random data will be used to store said second data set.

131. (Previously presented) The method according to claim 126 wherein the data storage area initialized with random data is reserved for use in storing data.

132. (Previously presented) The method according to claim 126 wherein the data storage area initialized with random data comprises a file of random data which is managed by a conventional file system on a computer.

133. (Previously presented) A removable storage device comprising a data storage area initialized with random data, wherein a file index and a data set are stored in the data storage area initialized with random data, the file index is encrypted and stored at a first location within the data storage area initialized with random data, the data set is encrypted and stored at a second location within the data storage area initialized with random data, the file index comprises an entry in respect of the data set, the entry comprising an indication of the second location within the data storage area initialized with random data, and the file index comprises an indication of which parts of the data storage area initialized with random data are in use to store said data set.

134. (Previously presented) A removable storage device carrying software and comprising a data storage area initialized with random data, the software comprising code portions which when loaded and run on a computer cause the computer to execute a method of storing a data set on the storage device, the method comprising the steps of:

selecting a first location within the data storage area initialized with random data for storing a file index;

selecting a second location within the data storage area initialized with random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the data storage area initialized with random data;

ensuring that an indication of the second selected location is determinable from the file index;

encrypting the file index; and

storing the encrypted file index at the first selected location in the data storage are initialized with random data, and comprising, before the step of encrypting the file index, a further step of recording in the file index an indication of which parts of the data storage area initialized with random data will be used to store said data set.

135. (New) A method of storing a data set on a storage device having one or more portions of random data, comprising:

determining a first storage writing process starting location at a first offset within a portion of random data for initiating a first storage writing process for storing a data set;

determining a second storage writing process starting location at a second offset within a portion of random data for initiating a second storage writing process that creates a file index, said second offset determined independently from a process used to generate the first offset;

encrypting the data set;

writing the encrypted data set using said first storage writing process beginning at said first storage writing process starting location;

creating a file index having an entry in respect of the data set, the entry comprising at least an indication of the first storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using said second storage writing process beginning at said second storage writing process starting location.

136. (New) The method of claim 135 wherein said second offset is determined using an algorithm that is dependent upon an input passphrase.